

TENT COOPERATION TRI Y

PCT

NOTIFICATION OF THE RECORDING
OF A CHANGE(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

From the INTERNATIONAL BUREAU

To:

KLETT, Peter, Michael
International Business Machines
Corporation
Säumerstrasse 4
CH-8803 Rüschlikon
SUISSE

Date of mailing (day/month/year)

20 December 1999 (20.12.99)

Applicant's or agent's file reference

SZ9-98-027

IMPORTANT NOTIFICATION

International application No.

PCT/IB98/01854

International filing date (day/month/year)

23 November 1998 (23.11.98)

1. The following indications appeared on record concerning:



the applicant



the inventor



the agent



the common representative

Name and Address

BINDING, Carl
Alpenstrasse 16
CH-8803 Rüschlikon
Switzerland

State of Nationality

CH

State of Residence

CH

Telephone No.

Facsimile No.

Teleprinter No.

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:



the person



the name



the address



the nationality



the residence

Name and Address

BINDING, Carl
Russistrasse 7
CH-8800 Thalwil
Switzerland

State of Nationality

State of Residence

Telephone No.

Facsimile No.

Teleprinter No.

3. Further observations, if necessary:

4. A copy of this notification has been sent to:



the receiving Office



the International Searching Authority



the International Preliminary Examining Authority



the designated Offices concerned



the elected Offices concerned



other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Authorized officer

J. Leitao

Facsimile No.: (41-22) 740.14.35

Telephone No.: (41-22) 338.83.38

TENT COOPERATION TRE Y

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 18 February 2000 (18.02.00)	
International application No. PCT/IB98/01854	Applicant's or agent's file reference SZ9-98-027
International filing date (day/month/year) 23 November 1998 (23.11.98)	Priority date (day/month/year) 15 July 1998 (15.07.98)
Applicant BINDING, Carl et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:
13 January 2000 (13.01.00)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was
☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

<p>The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland</p> <p>Facsimile No.: (41-22) 740.14.35</p>	<p>Authorized officer</p> <p>Jean-Marc Vivet</p> <p>Telephone No.: (41-22) 338.83.38</p>
--	--

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference SZ9-98-027	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/IB98/01854	International filing date (day/month/year) 23/11/1998	Priority date (day/month/year) 15/07/1998
International Patent Classification (IPC) or national classification and IPC H04L9/32		
Applicant INTERNATIONAL BUSINESS MACHINES CORPORATION et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.



2. This REPORT consists of a total of 7 sheets, including this cover sheet.

- ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 8 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 13/01/2000	Date of completion of this report 30.10.2000
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Chêne, X Telephone No. +49 89 2399 8266 

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/IB98/01854

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

3-11,13 as originally filed

1,2,2a-2b,12 as received on 01/09/2000 with letter of 30/08/2000

Claims, No.:

11 as originally filed

1-10 as received on 01/09/2000 with letter of 30/08/2000

Drawings, sheets:

1/1 as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

see separate sheet

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/IB98/01854

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-11
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-11
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-11
	No:	Claims	

2. Citations and explanations

see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/IB98/01854

Re Item I

Basis of the report

1. No examination of the amended claim 11 is possible since a part of the subject-matter is missing, so that the claim has no sense.
2. However, an opinion is given on the basis of the initial claim 11 as originally filed since the Applicant mentions in his letter of reply to the first opinion that only claims 1, 6 and 10 have been changed.

Re Item V

Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Reference is made to the following documents cited in the International Search Report:
D1: MOLVA, SAMFAT AND TSUDIK: 'Authentication of Mobile Users' IEEE NETWORK, vol. 8, no. 2, 1 April 1994, pages 26-34, XP000515077 NY, US,
D2: CHADWICK, YOUNG AND CICOVIC: 'Merging and Extending the PGP and PEM Trust Models-The ICE-TEL Trust Model' IEEE NETWORK, vol. 11, no. 3, 1 May 1997, pages 16-24, XP000689785 NY, US,
D3: US-A-5 371 794 (DIFFIE ET AL.) 6 December 1994,
D4: US-A-5 402 490 (MIHM, JR) 28 March 1995,
D5: EP-A-0 586 022 (FISCHER) 9 March 1994,
D6: C PARK: 'On Certificate-Based Security Protocols for Wireless Mobile Communication Systems' IEEE NETWORK, vol. 11, no. 5, 1 September 1997, pages 50-55, XP000699941 NY, US.
2. **The subject-matter of claim 1 appears to involve an inventive step** with regard to the known prior art shown in the International Search Report according to Article 33(3) PCT.

The present invention concerns a method of establishing a trustworthiness level of a participant in a communication connection between a first communication

partner and a second communication partner and for adapting communication behaviour to the established trustworthiness level. An important aspect of the invention is that, additionally to a mutual authentication process of a first communication partner and a participant, the first communication partner obtains the trust level of the participant and communicates it to the second participant, which adapts his behaviour according to the trust level of the participant.

Document D3, which is considered as the most relevant document, discloses a method for providing a secure wireless communication link between a mobile nomadic device and a base computing. The principle is based on a mutual recognition of certificates. No trust level of the base computing is mentioned.

The problem to be solved can be considered as how to introduce a level of trust in a participant to a communication between two partners. This is a known problem as illustrated for example by documents D5 or D2.

Document D5 discloses a public key/signature cryptosystem with digital signature certification field. Particularly, a certificate includes information about the level of trust granted to a certifiee (cf. page 4, lines 35-39). But document D5 does not disclose a solution where the first communication partner obtains the level of trust of the participant and sends it to the second communication partner.

The same remark applies also for document D2 (cited in the international search report as an "Y" document). The principle to adapt the communication behaviour according to information about the level of trust of a communication partner is mentioned (see page 21, right column, 4th paragraph), but it is not disclosed that a first communication partner obtains information about the level of trust of a participant and transmits it to a second communication partner in order to adapt the communication behaviour.

Document D1, cited as a document of particular relevance ("X"), discloses a set of inter-domain security mechanisms using electronic certificates and authentication procedure. However, document D1 does not consider the problem of level of trust of the participant to a communication. It does not provide more information than document D3.

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/IB98/01854

Consequently, for a person skilled in the art, the subject-matter of claim 1 appears to involve an inventive step, since no document of the prior art, taken alone or in combination with other document of the prior art or with general knowledge leads obviously to the subject-matter of claim 1.

3. **The subject-matter of independent claim 10 appears to involve an inventive step** with regard to the known prior art shown in the International Search Report according to Article 33(3) PCT.

A similar reasoning as in above point 2 for claim 1 applies also for claim 10 since it appears to define the same invention.

4. **The subject-matter of claims 2-9 and 11 (as originally filed), dependent on claims 1 or 10 appearing to be inventive, are consequently considered to involve an inventive step** with regard to the known prior art shown in the International Search Report according to Article 33(3) PCT.

Re Item VIII

Certain observations on the international application

1. The application does not fulfil the requirement of Article 6 PCT since **claims 1 and 10 are not concise**. These claims describe methods which have overlapping scope: claim 10 appears to be a generalisation of claim 1 ; instead of describing precisely, as in claim 1, the exchange of certificates and their mutual check which leads to the determination of a trustiness level, claim 10 summarizes it by an authentication test which also leads to establish a trustworthiness level.
2. The application does not fulfil the requirement of Article 6 PCT since **claim 1 is not clear** for the following reason:

In the expression "*at least one parameter of said communication behaviour is chosen in dependence of said established trustworthiness level*", the essential feature that the second communication partner chooses the communication behaviour does not clearly appear (see description, page 7, lines 6-11). Such

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/IB98/01854

feature is essential for the invention and has been pointed out by the Applicant in its letter of reply to the first communication.

3. The application does not fulfil the requirement of Article 6 PCT since **independent claim 10 is not clear** for the following reasons:

- i) Claim 10 attempts to define its subject-matter in terms of the result to be achieved (See PCT Preliminary Examination Guidelines III-4.7). In the expression "*an authentication test [...] which also leads to establishing said trustworthiness level*", there is no feature explaining how the trustworthiness level is established from the authentication test. Since the establishment of a trustworthiness level is not an obvious result of an authentication test, the corresponding technical features should be added to explain how this result is achieved.
- ii) The objection raised for claim 1 in point 2 applies also for claim 10.

4. The application does not fulfil the requirement of Article 6 PCT since **dependent claims 3 and 5 are not clear** for the following reason:

- i) In claim 3, the expression "*the certificate authority public key (17)*" lacks of antecedent. This expression is effectively not defined in claim 1 on which claim 3 depends, but in claim 2.
- ii) In claim 5, the expression "*the trustworthiness level information (TLT)*" lacks of antecedent. This expression is effectively not defined in claim 1 on which claim 5 depends, but in claim 4.

IPLZH 03FEB'00 16:38

PCT

From the INTERNATIONAL BUREAU

NOTICE INFORMING THE APPLICANT OF THE
COMMUNICATION OF THE INTERNATIONAL
APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:

KLETT, Peter, Michael
International Business Machines
Corporation
Säumerstrasse 4
CH-8803 Rüschlikon
SUISSE

Date of mailing (day/month/year) 27 January 2000 (27.01.00)		IMPORTANT NOTICE	
Applicant's or agent's file reference SZ9-98-027			
International application No. PCT/IB98/01854	International filing date (day/month/year) 23 November 1998 (23.11.98)	Priority date (day/month/year) 15 July 1998 (15.07.98)	
Applicant INTERNATIONAL BUSINESS MACHINES CORPORATION et al			

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:
CN,EP,JP,KR,US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
BR,CA

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on
27 January 2000 (27.01.00) under No. WO 00/04673

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a **demand for international preliminary examination** must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the **national phase**, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. (41-22) 740.14.35	Authorized officer J. Zahra Telephone No. (41-22) 338.83.38
--	---

METHOD OF ESTABLISHING THE TRUSTWORTHINESS LEVEL OF A PARTICIPANT IN A COMMUNICATION CONNECTION

The invention relates to a method for establishing a trustworthiness level of a participant in a communication connection between a first communication partner and a second communication partner. More particularly it relates to a method for establishing the trustworthiness level of a handheld device, such as a handheld telephone in a trusted environment, e.g. comprising a smartcard and a back-end server.

TECHNICAL FIELD AND BACKGROUND OF THE INVENTION

Integrated-circuit cards, also known as smartcards, are generally believed to offer more tamper resistance than conventional computer systems, and are thus frequently used for authentication and security functions within large computer systems. As an example, the use of a smartcard as the Subscriber Identification Module, short SIM, within the GSM mobile-telephony system is considered. Here, the mobile handset, also called mobile equipment or ME, is not normally considered as a trusted device and a trusted smartcard is used to securely store and process subscriber information and authentication functions. When placing a call, the mobile network authenticates the mobile user by exercising authentication functions contained in the trusted smartcard.

Handheld phones are currently being extended to allow user programs to be executed on the handheld phone for value-add applications such as banking and payment. Access to the smartcard of the handheld phone is provided for the relevant security functions required for a value-add application, such as the initial authentication for a financial transaction originating from the handset. While it is possible to have the smartcard perform all critical security functions, this is unlikely since the smartcard has limited processing- and storage capacity. It is thus anticipated that security functions for complex applications like banking will not be executed solely on the smartcard, and at least partial trust must be delegated to the handheld phone. Apart from issues of processing and storage, the smartcard must implicitly trust the handheld phone to provide a reliable communication channel to and from the smartcard.

Henceforth, it is anticipated that portions of complex applications will execute on the handheld phone. Since the handheld phone also conveys all communications between the

smartcard, the user, and the back-end server. a malicious handheld phone could conceivably alter the contents of the data packets sent between the three parties. Relying on the trusted smartcard to sign or authenticate messages does not alleviate this threat since the smartcard cannot verify that a message presented to it by the handheld phone for signature or authentication is in fact the message presented by the handheld phone to the user.

It is therefore necessary for applications that demand high levels of security and secrecy to extend the sphere of trust to include the handheld phone itself. Conventionally, this is achieved through two primary means, tamper-resistant hardware and ensuring that such tamper-resistant devices are being used through either policy or by authentication from the back-end server.

Designing special tamper-resistant hardware may involve special ruggedized designs with circuitry that erases security-sensitive information such as cryptographic parameters and aborts pending transactions if a device is physically tampered with, such as when the case is opened, or the power is cut, or designing hardwired circuits that do not have any software-controlled components on the paths between the trusted smartcard and the required input/output devices.

Unfortunately, mobile equipment such as mobile handsets are not currently designed to be tamperproof and adding full tamper-resistance is not realistic for commodity-style handsets due to the expected cost of doing so.

OBJECT AND ADVANTAGES OF THE INVENTION

It is an object of the invention according to claim 1 or 10 to provide a method for establishing the trustworthiness level of a participant in a communication connection in order to adapt the communication behavior to this trustworthiness level. Since the world of participants in communication is split up into tamperproof devices which can be trusted and devices which are better not trusted for security-sensitive communication, the invention provides an advantageous solution for communicating between two partners over a participant by establishing its trustworthiness level and adapting the communication behavior to the established trustworthiness level. With this method, trusted and non-trusted devices can participate in the communication and the trustworthiness of each participating device is checked automatically before communicating security-sensitive information.

behavior according to the trustworthiness level TL given in the trustworthiness level token TLT.

5 The smartcard 1 is then instructed by the user to establish a secure and authenticated session with the back-end server 3 so as to run the application A. The back-end server 3 and the smartcard 1 run WTLS using the option where both the client, i.e. the smartcard 1, and the back-end server 3 are authenticated using certificate exchange. At this point the trustworthi-
ness between the back-end server 3 and smartcard 1 has been established.

10 When the smartcard 1 is required to send application data D to the back-end server 3, the smartcard 1 appends the trustworthiness level token TLT and sends the pair (D, TLT). Since the channel between the back-end server 3 and the smartcard 1 is authenticated, the back-end server 3 believes that the trustworthiness level TL given in the trustworthiness level token TLT is in fact the trustworthiness level TL of the handheld phone 2 hosting the smart-
card 1 for this session.

15 The trustworthiness level token TLT is a data item which is meaningful to the back-end server 3. It could be identical with the integer value of the trustworthiness level TL, in which case the back-end server 3 shall examine the policy 16 that describes its actions or communication behavior for that trustworthiness level TL. Alternatively, the trustworthiness level token TLT could directly denote the intended trustworthiness level TL according to some relevant trustworthiness metric e.g. monetary amount. Then, no policy 16 is needed.

20 This example also makes the authentication step between the smartcard 1 and the back-end server 3 explicit, but this need not always be the case. If the handheld phone 2 is a GSM handset, then the smartcard 1 may be a SIM which is authenticated at the time of insertion into the handset 2 using the standard GSM authentication algorithms. The base station of the SIM could forward this authentication information to the back-end server 3, and thus elimi-
25 nate the need for the establishment of WTLS session between the back-end server 3 and the SIM.

Another example id when the participant 2 does simply have stored the participant private key 8 and has no trustworthiness certificate 6. Then, the smartcard 1 can know either the participant private key 8 or the corresponding participant public key 7 and perform the
30 above described challenge-response test to find out whether the handheld phone 2 knows the participant private key 8. If this is the case, then a corresponding trustworthiness level TL

CLAIMS

1. Method of establishing a trustworthiness level (TL) of a participant (2) in a communication connection between a first communication partner (1) and a second communication partner (3) and for adapting communication behaviour to the established trustworthiness level (TL), whereby said participant (2) is equipped with a trustworthiness certificate (6) and a therefrom separated securely stored participant private key (8) and that said first communication partner (1) receives said trustworthiness certificate (6) from said participant (2), wherefrom said trustworthiness level (TL) is derived and established and said first communication partner (1) tests whether said trustworthiness certificate (6) belongs to said participant (2) using said participant private key (8) and that in case said trustworthiness certificate (6) is confirmed by said test to belong to said participant (2), said first communication partner (1) communicates said established trustworthiness level (TL) to said second communication partner (3) and that at least one parameter of said communication behaviour is chosen in dependence of said established trustworthiness level (TL).
2. Method according to claim 1, characterized in that the trustworthiness certificate (6) arrives at the first communication partner (1) signed with a signature (9), produced with a certificate authority private key, and that said first communication partner (1) authenticates said signature (9) using a certificate authority public key (17).
3. Method according to claim 2, characterized in that the certificate authority public key (17) is read from a storage of the first communication partner (1).
4. Method according to one of claims 1 to 3, characterized in that the first communication partner (1) communicates the established trustworthiness level (TL) to the second communication partner (2) by piggy-backing a trustworthiness level information (TLT) onto a communication message, signing said communication message with a first-partner private key (13) and sending it to said second communication partner (3).

5. Method according to claim 4, characterized in that the authenticity of the trustworthiness level information (TLT) of the communication message is testable by the second communication partner (3) by using a first-partner public key (11).
6. Method according to one of claims 1 to 5, characterized in that as one of the parameters of the communication behaviour which is chosen in dependence of the established trustworthiness level (TL), is chosen the amount or number of a valuable asset, e.g. a maximum number of financial transactions and/or a maximum financial value of a financial transaction and/or a maximum number of confidential words.
7. Method according to one of claims 1 to 6, characterized in that the test whether the trustworthiness certificate (6) belongs to the participant (2) is performed in that a test number (R_1) is transmitted by the first communication partner (1) to said participant (2) from where said test number (R_1) returns signed under use of the participant private key (8) and in that the signature of the returning test number (R_1) is verified by using a participant public key (7) which corresponds to said participant private key (8).
8. Method according to claim 7, characterized in that the participant public key (7) is received by the first communication partner (1) as content of the trustworthiness certificate (6).
9. Method according to claim 7 or 8, characterized in that the trustworthiness level (TL) is established in that for each trustworthiness level (TL) a different trustworthiness certificate (6) with a corresponding pair of participant public key (7) and participant private key (8) is used.

10. Method of establishing the trustworthiness level (TL) of a participant (2) in a communication connection between a first communication partner (1) and a second communication partner (3) and for adapting communication behaviour to the established trustworthiness level (TL), whereby said participant (2) is equipped with a securely stored participant private key (8) and that said first communication partner (1) performs an authentication test using said participant private key (8) which also leads to establishing said trustworthiness level (TL) and that in case of a successful authentication said first communication partner (1) communicates the established trustworthiness level (TL) to said second communication partner (3) and that at least one parameter of said communication behaviour is chosen in dependence of said established trustworthiness level (TL).
11. Method of establishing the trustworthiness level (TL) according to claim 10, characterized in that the authentication test is performed in that a test number (R_1) is transmitted by the first communication partner (1) to the participant (2) from where said test number (R_1) returns signed under use of the participant private key (8) and in that the signature of the returning test number (R_1) is verified by using a participant public key (7) which corresponds to said participant private key (8).

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference SZ9-98-027	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/IB 98/01854	International filing date (day/month/year) 23/11/1998	(Earliest) Priority Date (day/month/year) 15/07/1998
Applicant INTERNATIONAL BUSINESS MACHINES CORPORATION et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. ☐ **Certain claims were found unsearchable** (See Box I).

3. ☐ **Unity of invention is lacking** (see Box II).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No.

☒ as suggested by the applicant.

☐ because the applicant failed to suggest a figure.

☐ because this figure better characterizes the invention.

1
☐ None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/IB 98/01854

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 6 H04L9/32 H04Q7/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MOLVA, SAMFAT AND TSUDIK: "Authentication of Mobile Users" IEEE NETWORK, vol. 8, no. 2, 1 April 1994, pages 26-34, XP000515077 NY, US	1-3
A	see page 30, line 1 - page 34, line 42; figures 3-6	4-9
Y	CHADWICK, YOUNG AND CICOVIC: "Merging and Extending the PGP and PEM Trust Models-The ICE-TEL Trust Model" IEEE NETWORK, vol. 11, no. 3, 1 May 1997, pages 16-24, XP000689785 NY, US	1-3
A	see page 21, line 54 - page 24, line 19; figures 3-5	4-9



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

16 March 1999

Date of mailing of the international search report

24/03/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Authorized officer

Geoghegan, C

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/IB 98/01854

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 371 794 A (DIFFIE ET AL.) 6 December 1994	1-3
A	see column 3, line 46 - column 15, line 61; figures ---	4-9
A	US 5 402 490 A (MIHM, JR) 28 March 1995 see column 3, line 29 - column 12, line 49; figures ---	1-9
A	EP 0 586 022 A (FISCHER) 9 March 1994 see page 7, line 22 - page 20, line 51; figures ---	1-3
A	C PARK: "On Certificate-Based Security Protocols for Wireless Mobile Communication Systems" IEEE NETWORK, vol. 11, no. 5, 1 September 1997, pages 50-55, XP000699941 NY, US see page 51, line 1 - page 55, line 59; figures -----	1-3

INTERNATIONAL SEARCH REPORT

ation on patent family members

national Application No

PCT/IB 98/01854

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5371794	A	06-12-1994	EP	0651533 A	03-05-1995
			JP	7193569 A	28-07-1995

US 5402490	A	28-03-1995	NONE		

EP 586022	A	09-03-1994	US	5005200 A	02-04-1991
			AT	113429 T	15-11-1994
			AT	150605 T	15-04-1997
			AU	620291 B	13-02-1992
			AU	4242589 A	13-09-1990
			CA	2000400 A,C	07-09-1990
			DE	69013541 D	01-12-1994
			DE	69013541 T	09-03-1995
			DE	69030268 D	24-04-1997
			DE	69030268 T	26-06-1997
			DK	386867 T	03-04-1995
			EP	0386867 A	12-09-1990
			ES	2036978 T	01-01-1995
			ES	2098651 T	01-05-1997
			GR	93300050 T	30-06-1993
			JP	2291043 A	30-11-1990
			US	5214702 A	25-05-1993

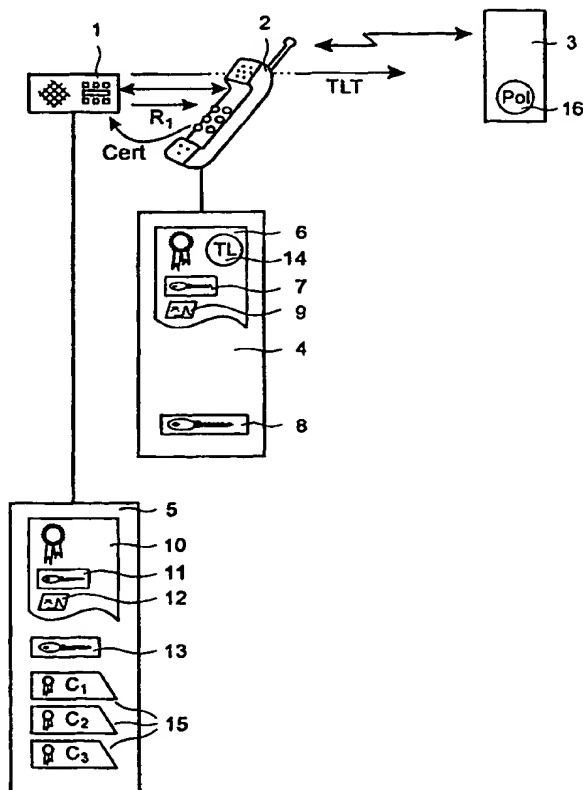
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L 9/32, H04Q 7/22		A1	(11) International Publication Number: WO 00/04673
			(43) International Publication Date: 27 January 2000 (27.01.00)
(21) International Application Number: PCT/IB98/01854		(81) Designated States: BR, CA, CN, JP, KR, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) International Filing Date: 23 November 1998 (23.11.98)			
(30) Priority Data: 98113121.2 15 July 1998 (15.07.98) EP		Published With international search report.	
(71) Applicant (for all designated States except US): INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, NY 10504 (US).			
(72) Inventors; and (75) Inventors/Applicants (for US only): BINDING, Carl [CH/CH]; Russistrasse 7, CH-8800 Thalwil (CH). HILD, Stefan, G. [DE/CH]; Austrasse 27, CH-8134 Adliswil (CH). MOSER, Michael [AT/CH]; Frohburgstrasse 19, CH-8006 Zurich (CH). O'CONNOR, Luke, J. [AU/CH]; Sihlhof 16, CH-8134 Adliswil (CH).			
(74) Agent: KLETT, Peter, Michael; International Business Machines Corporation, Säumerstrasse 4, CH-8803 Rüschlikon (CH).			

(54) Title: METHOD OF ESTABLISHING THE TRUSTWORTHINESS LEVEL OF A PARTICIPANT IN A COMMUNICATION CONNECTION

(57) Abstract

A method of establishing a trustworthiness level of a participant in a communication connection between a first communication partner and a second communication partner is proposed whereby the communication behavior is adapted to the established trustworthiness level. The participant is equipped with a trustworthiness certificate and a therefrom separated securely stored participant private key. The first communication partner receives the trustworthiness certificate from the participant wherefrom the trustworthiness level is derived and established. The first communication partner tests whether the trustworthiness certificate belongs to the participant by using the participant private key. In case the trustworthiness certificate is confirmed by the test to belong to the participant, the first communication partner communicates the established trustworthiness level to the second communication partner. Then, at least one parameter of the communication behavior is chosen in dependence of the established trustworthiness level.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD OF ESTABLISHING THE TRUSTWORTHINESS LEVEL OF A PARTICIPANT IN A COMMUNICATION CONNECTION

The invention relates to a method for establishing a trustworthiness level of a participant in a communication connection between a first communication partner and a second communication partner. More particularly it relates to a method for establishing the trustworthiness level of a handheld device, such as a handheld telephone in a trusted environment, e.g. comprising a smartcard and a back-end server.

TECHNICAL FIELD AND BACKGROUND OF THE INVENTION

Integrated-circuit cards, also known as smartcards, are generally believed to offer more tamper resistance than conventional computer systems, and are thus frequently used for authentication and security functions within large computer systems. As an example, the use of a smartcard as the Subscriber Identification Module, short SIM, within the GSM mobile-telephony system is considered. Here, the mobile handset, also called mobile equipment or ME, is not normally considered as a trusted device and a trusted smartcard is used to securely store and process subscriber information and authentication functions. When placing a call, the mobile network authenticates the mobile user by exercising authentication functions contained in the trusted smartcard.

Handheld phones are currently being extended to allow user programs to be executed on the handheld phone for value-add applications such as banking and payment. Access to the smartcard of the handheld phone is provided for the relevant security functions required for a value-add application, such as the initial authentication for a financial transaction originating from the handset. While it is possible to have the smartcard perform all critical security functions, this is unlikely since the smartcard has limited processing- and storage capacity. It is thus anticipated that security functions for complex applications like banking will not be executed solely on the smartcard, and at least partial trust must be delegated to the handheld phone. Apart from issues of processing and storage, the smartcard must implicitly trust the handheld phone to provide a reliable communication channel to and from the smartcard.

Henceforth, it is anticipated that portions of complex applications will execute on the handheld phone. Since the handheld phone also conveys all communications between the

smartcard, the user, and the back-end server, a malicious handheld phone could conceivably alter the contents of the data packets sent between the three parties. Relying on the trusted smartcard to sign or authenticate messages does not alleviate this threat since the smartcard cannot verify that a message presented to it by the handheld phone for signature or authentication is in fact the message presented by the handheld phone to the user.

It is therefore necessary for applications that demand high levels of security and secrecy to extend the sphere of trust to include the handheld phone itself. Conventionally, this is achieved through two primary means, tamper-resistant hardware and ensuring that such tamper-resistant devices are being used through either policy or by authentication from the back-end server.

Designing special tamper-resistant hardware may involve special ruggedized designs with circuitry that erases security-sensitive information such as cryptographic parameters and aborts pending transactions if a device is physically tampered with, such as when the case is opened, or the power is cut, or designing hardwired circuits that do not have any software-controlled components on the paths between the trusted smartcard and the required input/output devices.

Unfortunately, mobile equipment such as mobile handsets are not currently designed to be tamperproof and adding full tamper-resistance is not realistic for commodity-style handsets due to the expected cost of doing so.

OBJECT AND ADVANTAGES OF THE INVENTION

It is an object of the invention according to claim 1 or 10 to provide a method for establishing the trustworthiness level of a participant in a communication connection in order to adapt the communication behavior to this trustworthiness level. Since the world of participants in communication is split up into tamperproof devices which can be trusted and devices which are better not trusted for security-sensitive communication, the invention provides an advantageous solution for communicating between two partners over a participant by establishing its trustworthiness level and adapting the communication behavior to the established trustworthiness level. With this method, trusted and non-trusted devices can participate in the communication and the trustworthiness of each participating device is checked automatically before communicating security-sensitive information.

The participant can e.g. be a mobile equipment such as a handheld phone. The trustworthiness level of the handheld phone indicates the degree of inherent tamper resistance. The first communication partner can be for instance a smartcard and the second communication partner a back-end server.

- 5 The smartcard can use the handheld phone to connect to a back-end server, and the smartcard and the back-end server are in an advantageous manner able to establish an authenticated session, assuming an untrusted handheld phone. After establishing the trustworthiness level, the smartcard communicates the trustworthiness level of the handheld phone to the back-end server without the back-end server directly authenticating the handheld phone.
- 10 It is another object to provide a method where a trustworthiness policy is specified for an application, which policy restricts the functionality of the application based on the trustworthiness level of the handheld phone.

- When the trustworthiness certificate arrives at the first communication partner signed with a signature, produced with a certificate authority private key, and the first communication
- 15 partner authenticates the signature using a certificate authority public key, a secure method is used to check whether the signature has been issued by a competent and to-be-trusted certificate authority. This is advantageous because it then can easily be confirmed that the information contained in the corresponding participant certificate is as issued by its originator.

- 20 The certificate authority public key can be read from a storage of the first communication partner, which has the advantage that this key is already available and need not be acquired from somewhere else. This also saves time.

- Communicating the detected trustworthiness level can occur by piggybacking and signing necessary information onto application level messages between the smartcard and the back-
- 25 end, application server. When the first communication partner communicates the established trustworthiness level to the second communication partner by piggy-backing a trustworthiness level information onto a communication message, signing the communication message with a first-partner private key and sending it to the second communication partner, again a very secure way of informing the back-end server about the established trustworthiness level

is chosen. Hence, a malicious participant can not amend this information and thereby pretend to be a trustable participant.

As one of the parameters of the communication behavior which is chosen in dependence of the established trustworthiness level, can be chosen the amount or number of a valuable asset, e.g. a maximum number of financial transactions and/or a maximum financial value of a financial transaction and/or a maximum number of confidential words. This adapted behavior can be used to compensate for eventual lack of security which has been established in form of a low trustworthiness level. For instance, in case of a low trustworthiness level, only financial transactions up to a fixed amount of money can be executed.

10 The test whether the trustworthiness certificate belongs to the participant can be performed in that a test number is transmitted by the first communication partner to the participant from where the test number returns signed under use of the participant private key. The signature of the returning test number is verified by using a participant public key which corresponds to the participant private key. This challenge-response principle provides a simple method which is easy to implement and provides a high level of security.

The participant public key can be received by the first communication partner as content of the trustworthiness certificate. This method provides for the possibility of multiple trustworthiness certificates and hence also multiple trustworthiness levels, if each certificate is assigned a different trustworthiness level.

20 When the trustworthiness level is established in that for each trustworthiness level a different trustworthiness certificate with a corresponding pair of participant public key and participant private key is used, a very simple and straightforward scheme for realizing different levels is provided. It can be used in that e.g. for different key lengths or just different signing authorities, different trustworthiness levels can be assigned.

25 The handheld phone is providing communication- and processing resources for the smart-card and the back-end server to execute an application. The back-end server wishes to authenticate the handheld phone since security-sensitive data may be sent to the smartcard via the handheld phone. As the handheld phone and the back-end server may be separated by a substantial physical distance and/or connected by a low-bandwidth network, running a traditional authentication protocol between the handheld phone and the back-end server may be costly. It is hence more efficient to make use of the smartcard to authenticate the

trustworthiness level of the handheld phone locally where communication between the smartcard and handheld phone is relatively fast and cheap.

The proposed solution is most advantageous to the deployment of banking services based on mobile handsets, for example GSM telephones, since such applications demand high levels of security. As pointed out above, this in turn requires some trustworthiness level to be extended to the handset itself. Not all handsets will be trusted, due to the cost of designing and manufacturing such handsets and due to the large number of handsets which are already in-the-field that do not include any tamper-resistance.

The smartcard acts as a sort of delegate or proxy for the back-end server which establishes the trustworthiness level locally with respect to the handheld-phone/smartcard environment. The system described herein allows the trusted smartcard to detect the level of tamper-resistance of the handheld phone and communicate that level to the back-end server. An inherent advantage of the proposed solution compared to server-based device authentication methods lies in the reduced communications requirement between the back-end server and the handheld phone which lowers communications cost on one side and allows the process to be executed repeatedly if necessary, e.g., prior to each message between the smartcard and the back end server, offering additional protection.

Adapting the application behavior to the communicated trustworthiness level can be implemented by limiting the number of transactions or establishing a maximum financial value of the executed transactions. For example, from completely untrusted handsets only account inquiries might be allowed, whereas completely trusted handsets can be used to execute arbitrarily large value transactions. Handsets that offer intermediate levels of trustworthiness might be limited to transactions up to a certain value per month.

SUMMARY OF THE INVENTION

A method is proposed whereby a trustworthiness level is assigned to a handheld phone, that reflects the level of tamper-resistance that the handheld phone offers. Current mobile handsets, for example, offer no tamper-resistance and would be assigned the lowest trustworthiness level. Future fully tamperproof handsets would be assigned the highest trustworthiness level. Intermediate trustworthiness levels would designate for which incomplete but not insignificant measures against tampering have been made.

The first communication partner, e.g. a smartcard, has means of verifying the level of tamper-resistance of the handheld phone which is a participant in the communication connection between the first communication partner and a second communication partner and further has means to securely communicate the detected level of tamper-resistance in the
5 handheld phone to the second communication partner, e.g. a back-end server with whom the smartcard is communicating during the execution of an application on the participant.

The back-end server is then able to adapt the behavior of the communication, respectively application according to the level of tamper-resistance detected and communicated to it by the smartcard.

10 The basic steps of the method can be described as follows:

When the smartcard is inserted into the handheld phone to initiate a session, the smartcard requests the trustworthiness level from the handheld phone. The trustworthiness level may be assigned for example by the manufacturer of the handheld phone or perhaps by the institution with which applications on the handheld phone will communicate with or on behalf of,
15 such as a bank or credit card company.

The smartcard verifies that the trustworthiness level received from the handheld phone is valid in the sense that the token was produced by an entity with the authority to assign trustworthiness levels and also that the trustworthiness level is not being replayed. If the trustworthiness level fails verification then the handheld phone is considered untrusted. If this is
20 the case, the smartcard may choose to terminate the session, or continue the session with the restriction that only applications requiring an untrusted handheld phone can be executed. The smartcard then forms a trustworthiness level token TLT which the smartcard will use to forward to third parties to demonstrate the trustworthiness level of the handheld phone.

An application on the handheld phone is selected for execution, where the application uses
25 the network to contact a back-end server. The back-end server and the smartcard are authenticated to each other using a protocol that does not depend on the trustworthiness of the handheld phone. For example, if the handheld phone is a GSM handset and the smartcard is a SIM, then the back-end server and the smartcard SIM are authenticated using the standard GSM authentication functions. Alternatively the authentication functions of WTLS
30 can be used.

The smartcard communicates the trustworthiness level of the handheld phone to the back-end server by appending the trustworthiness level token TLT to the application packets of the application that are sent from the smartcard to the back-end server S. The trustworthiness level token TLT may be appended to each packet or according to another strategy
5 depending on some policy.

Once the back-end server has received the trustworthiness level token TLT of the handheld phone via the smartcard, it need not verify the trustworthiness level of the handheld phone with the handheld phone itself, as this has been done by the trusted smartcard. The back-end server consults a trustworthiness policy which describes what restrictions are placed on
10 application relative to the trustworthiness level designated by trustworthiness level token TLT. The back-end server adjusts its actions and responses in application accordingly.

DESCRIPTION OF THE DRAWINGS

An example of the invention is depicted in the drawing and described in detail below by way of example. It is shown in fig. 1 a system with a first communication partner, a participant
15 and a second communication partner.

The figure is for sake of clarity not shown in real dimensions, nor are the relations between the dimensions shown in a realistic scale.

DETAILED DESCRIPTION OF THE INVENTION

In the following, the various exemplary embodiments of the invention are described.

20 In figure 1, a system comprising a first communication partner 1 in form of a smartcard, a second communication partner in form of a back-end server 3 and a participant 2 in a communication connection between the communication partners 1, 3 in form of a handheld phone is depicted. The handheld phone 2 comprises a memory unit 4, also called phone trustworthiness module, in which a trustworthiness certificate 6 is stored.

25 When the smartcard 1 is inserted into the handheld phone 2 to initiate a session via the communication connection, the smartcard 1 requests the transmission of the trustworthiness certificate 6 from the handheld phone 2.

The following realization is based on the use of the principle of public key cryptography, which enables an entity to produce a digital signature and other entities to verify the signature. Other authentication methods however apply as well.

It is assumed that the valid set of trustworthiness levels TL is represented by a list of $L+1$ integers 0, 1, ..., L, such that 0 designates no trustworthiness, 1 designates minimum trustworthiness and L designates maximum trustworthiness. The values between 0 and L represent intermediate trustworthiness levels TL, where a higher value implies higher trustworthiness.

At the time of production or personalization, the phone trustworthiness module 4 was loaded with the trustworthiness certificate 6 $\text{Cert}_{\text{CA}}^{\text{ME}}$, for example in X509 format or in WTLS format. The trustworthiness certificate 6 $\text{Cert}_{\text{CA}}^{\text{ME}}$ represents a binding between the name of the handheld phone 2, and a participant public key 7 K_{ME} , which binding is described in the trustworthiness certificate 6 $\text{Cert}_{\text{CA}}^{\text{ME}}$. The trustworthiness certificate 6 $\text{Cert}_{\text{CA}}^{\text{ME}}$ also contains an extension field 14 containing an integer which gives the trustworthiness level TL assigned to the handheld phone 2, where $0 \leq TL \leq L$. The trustworthiness certificate 6 bears trustworthiness certificate signature 9 from a certificate authority CA, which therefor used its certificate authority private key.

A participant private key 8 K_{ME}^{-1} associated with the participant public key 7 K_{ME} of the trustworthiness certificate 6 and functions that operate using that participant private key K_{ME}^{-1} are also loaded into the phone trustworthiness module 4 of the handheld phone 2, which module 4 is a secure and tamperproof processing area. Such an area should be used in all handheld phones with a trustworthiness level TL greater than 0. At least the participant private key 8 K_{ME}^{-1} need be securely stored, i.e. such that it can not be read by a non-allowed person or device.

Thus, the handheld phone 2 has assigned a participant public/private key pair 7, 8 $K_{\text{ME}}/K_{\text{ME}}^{-1}$ which can be used for verifying the affiliation or belonging of the trustworthiness certificate 6 to the handheld phone 2. The handheld phone 2 contains the signed trustworthiness certificate 6 that contains its participant public key 7 and also the trustworthiness level TL assigned to the handheld phone 2.

A certificate authority public key 17 corresponding to the certificate authority private key can be deemed to be publicly available, such that any entity can use it to check the

trustworthiness certificate signature 9 and therewith the affiliation of the handheld phone 2 and the trustworthiness certificate 6. Hence the trustworthiness level TL can be determined. Otherwise, the certificate authority might also provide the first communication partner 1 with this certificate authority public key 17, or it can be downloaded from somewhere, e.g. a data network.

At the time of production or personalization, a smartcard module 5 of the smartcard 1 is loaded with a first-partner certificate 10 Cert_{CA}^{SC} designating a first-partner public key 11 K_{SC} for the smartcard 1 and a first-partner certificate signature 12. An associated first-partner private key 13 K_{SC}^{-1} is also loaded into the smartcard trustworthiness module 5, along with a collection 15 of three sample certificates C_1, C_2, C_3 of various certification authorities CA_1, CA_2, CA_3 . Three sample certificates have been chosen for sake of exemplarity only. The collection 15 of sample certificates should generally be sufficiently large so that the trustworthiness certificate 6 Cert_{CA}^{ME} presented by an arbitrary handheld phone 2 can be verified with very high probability. Here, a first sample certificate C_1 of the sample certificates C_1, C_2, C_3 contains the certificate authority public key 17 needed for authenticating or verifying the trustworthiness certificate signature 9.

When the smartcard 1 is now placed into the handheld phone 2, the trustworthiness level TL of the handheld phone 2 can be established as follows:

The smartcard 1 generates a random number R_1 and transmits it to the phone trustworthiness module 4 of the handheld phone 2. This is also called a challenge step, which is supposed to effect a response by the handheld phone 2.

The phone trustworthiness module 4 of the handheld phone 2 signs the random number R_1 with its participant private key 8 K_{ME}^{-1} , and returns the signature $\text{Sign}(R_1)$ for the random number R_1 together with its trustworthiness certificate 6 Cert_{CA}^{ME} to the smartcard 1.

The smartcard 1 searches through its collection 15 of certificates C_1, C_2, C_3 to find the first sample certificate C_1 for the certificate authority CA, and verifies the trustworthiness certificate signature 9 on the received trustworthiness certificate 6 Cert_{CA}^{ME} . Concerning the collection 15 of certificates C_1, C_2, C_3 , it is possible to preload a preselection of such certificates on the smartcard 1 to cover the most popular certificate authorities CA. Whenever the trustworthiness certificate signature 9 does not have its equivalent certificate authority public key 17 and the thereto belonging certificate in the smartcard 1, the missing certificate

can be loaded from a source which provides this certificate, e.g. some network. It is usual that certificates are arranged in form of chains which means that for trusting a certificate its signature is to be tested wherefor a public key, embedded in another certificate is used, which other certificate is again signed, which signature is again to be checked, a.s.o. until
5 one arrives at a definitely to be trusted certification authority, e.g. oneself. Also several of such certificate chains can exist.

If the trustworthiness certificate signature 9 is correct, the smartcard 1 then extracts the participant public key 7 K_{ME} from the trustworthiness certificate 6 $Cert^{ME}_{CA}$ and verifies therewith the random-number signature $Sign(R_1)$. The smartcard 1 aborts the process if
10 either signature verification fails and establishes a trustworthiness level TL of 0.

If the verification succeeds, the smartcard 1 examines the trustworthiness field 14 in the trustworthiness certificate $Cert^{ME}_{CA}$ and constructs a trustworthiness level token (TLT) which indicates that the handheld phone 2 which is hosting the smartcard 1 has been authenticated by the smartcard 1 to the trustworthiness level TL.

15 The smartcard 1 has hence verified that the received trustworthiness certificate $Cert^{ME}_{CA}$ is valid in the sense that it was produced by an entity with the authority to assign the trustworthiness certificate $Cert^{ME}_{CA}$ and also that the trustworthiness certificate $Cert^{ME}_{CA}$ is not being replayed or imitated.

If the trustworthiness certificate 6 $Cert^{ME}_{CA}$ fails verification then the handheld phone 2 is
20 considered untrusted, i.e. it is assigned a trustworthiness level TL of 0. In this case, the smartcard 1 may choose to terminate the session, or continue the session with the restriction that only applications which are allowed to run on the non-secure communication connection can be executed.

The smartcard 1 creates the trustworthiness level token TLT which represents the established trustworthiness level TL and forwards it to the second communication partner 3,
25 which is a third party, to demonstrate to this third party the trustworthiness level TL of the handheld phone 2.

The smartcard 1 can communicate the established trustworthiness level TL to the second communication partner 3 by piggy-backing the trustworthiness level information TLT onto a
30 communication message, signing this communication message with the first-partner private

key 13 and sending it to the second communication partner 3 where the signature can be tested by using the first-partner public key 11.

Alternatively, as e.g. used in GSM, the two communication partners 1, 3 can already trust each other before establishing the trustworthiness level TL of the participant 2 in that they both have a common private key, which could be the first-partner private key 13. This can be realized in that the smartcard 1 is issued by an authority which has set up the first-partner private key 13 in the server 3 and in that the smartcard is by this authority, which then of course is to be trusted, preloaded with the first-partner private key 13.

An application which uses contact to the back-end server 3 and which runs on the handheld phone 2 is selected for execution. The back-end server 3 and the smartcard 1 are authenticated to each other using a protocol that does not depend on the trustworthiness of the handheld phone 2. For example, if the handheld phone 2 is a GSM handset and the smartcard 1 is a SIM, then the back-end server 3 and the smartcard 1 are authenticated using the standard GSM authentication functions. Alternatively the authentication functions of WTLS can be used.

The smartcard 1 communicates the trustworthiness level TL of the handheld phone 2 to the back-end server 3 by appending the trustworthiness level token TLT to the application packets of the application that are sent from the smartcard 1 to the back-end server 3. The trustworthiness level token TLT may be appended to each application packet or be transmitted according to another strategy, depending on a determined token communication policy, e.g. once per a fixed time period or a fixed number of times per session etc.

When the back-end server 3 has received the trustworthiness level token TLT of the handheld phone 2 via the smartcard 1, it need not verify the trustworthiness level TL of the handheld phone 2 with the handheld phone 2 itself, because this has already been done by the trusted smartcard 1. For the application A the back-end server 3 consults a trustworthiness policy 16 pol(A), e.g. in form of a stored table, which describes what restrictions are placed on the application A relative to the trustworthiness level TL designated by the trustworthiness level token TLT. The back-end server 3 adjusts its actions and responses in the application A accordingly. With other words, the back-end server 3 consults the trustworthiness policy 16 pol(A) for the application A, and modifies or chooses its communication

behavior according to the trustworthiness level TL given in the trustworthiness level token TLT.

The smartcard 1 is then instructed by the user to establish a secure and authenticated session with the back-end server 3 so as to run the application A. The back-end server 3 and the smartcard 1 run WTLS using the option where both the client, i.e. the smartcard 1, and the back-end server 3 are authenticated using certificate exchange. At this point the trustworthi-
5 ness between the back-end server 3 and smartcard 1 has been established.

When the smartcard 1 is required to send application data D to the back-end server 3, the smartcard 1 appends the trustworthiness level token TLT and sends the pair (D, TLT). Since
10 the channel between the back-end server 3 and the smartcard 1 is authenticated, the back-end server 3 believes that the trustworthiness level TL given in the trustworthiness level token TLT is in fact the trustworthiness level TL of the handheld phone 2 hosting the smartcard 1 for this session.

The trustworthiness level token TLT is a data item which is meaningful to the back-end server 3. It could be identical with the integer value of the trustworthiness level TL, in which
15 case the back-end server 3 shall examine the policy 16 that describes its actions or communication behavior for that trustworthiness level TL. Alternatively, the trustworthiness level token TLT could directly denote the intended trustworthiness level TL according to some relevant trustworthiness metric e.g. monetary amount. Then, no policy 16 is needed.

20 This example also makes the authentication step between the smartcard 1 and the back-end server 3 explicit, but this need not always be the case. If the handheld phone 2 is a GSM handset, then the smartcard 1 may be a SIM which is authenticated at the time of insertion into the handset 2 using the standard GSM authentication algorithms. The base station of the SIM could forward this authentication information to the back-end server 3, and thus elimi-
25 nate the need for the establishment of WTLS session between the back-end server 3 and the SIM.

Another example id when the participant 2 does simply have stored the participant private key 8 and has no trustworthiness certificate 6. Then, the smartcard 1 can know either the participant private key 8 or the corresponding participant public key 7 and perform the
30 above described challenge-response test to find out whether the handheld phone 2 knows the participant private key 8. If this is the case, then a corresponding trustworthiness level TL

can be assigned. Different trustworthiness levels TL can correspond to different participant private keys 8.

In the above description, the untrusted party is a phone handset. It is to be noted that the general untrusted device is simply any mobile equipment, of which a mobile handset is an
5 example.

CLAIMS

1. Method of establishing a trustworthiness level (TL) of a participant (2) in a communication connection between a first communication partner (1) and a second communication partner (3) and for adapting communication behaviour to the established trustworthiness level (TL), whereby said participant (2) is equipped with a trustworthiness certificate (6) and a therefrom separated securely stored participant private key (8) and that said first communication partner (1) receives said trustworthiness certificate (6) from said participant (2), wherefrom said trustworthiness level (TL) is derived and established and said first communication partner (1) tests whether said trustworthiness certificate (6) belongs to said participant (2) using said participant private key (8) and that in case said trustworthiness certificate (6) is confirmed by said test to belong to said participant (2), said first communication partner (1) communicates said established trustworthiness level (TL) to said second communication partner (3) and that at least one parameter of said communication behaviour is chosen in dependence of said established trustworthiness level (TL).
2. Method according to claim 1, characterized in that the trustworthiness certificate (6) arrives at the first communication partner (1) signed with a signature (9), produced with a certificate authority private key, and that said first communication partner (1) authenticates said signature (9) using a certificate authority public key (17).
3. Method according to claim 2, characterized in that the certificate authority public key (17) is read from a storage of the first communication partner (1).
4. Method according to one of claims 1 to 3, characterized in that the first communication partner (1) communicates the established trustworthiness level (TL) to the second communication partner (2) by piggy-backing a trustworthiness level information (TLT) onto a communication message, signing said communication message with a first-partner private key (13) and sending it to said second communication partner (3).

5. Method according to claim 4, characterized in that the authenticity of the trustworthiness level information (TLT) of the communication message is testable by the second communication partner (3) by using a first-partner public key (11).
- 5 6. Method according to one of claims 1 to 5, characterized in that as one of the parameters of the communication behaviour which is chosen in dependence of the established trustworthiness level (TL), is chosen the amount or number of a valuable asset, e.g. a maximum number of financial transactions and/or a maximum financial value of a financial transaction and/or a maximum number of confidential words.
- 10 7. Method according to one of claims 1 to 6, characterized in that the test whether the trustworthiness certificate (6) belongs to the participant (2) is performed in that a test number (R_i) is transmitted by the first communication partner (1) to said participant (2) from where said test number (R_i) returns signed under use of the participant private key (8) and in that the signature of the returning test number (R_i) is verified by using a participant public key (7) which corresponds to said participant private key (8).
- 15 8. Method according to claim 7, characterized in that the participant public key (7) is received by the first communication partner (1) as content of the trustworthiness certificate (6).
- 20 9. Method according to claim 7 or 8, characterized in that the trustworthiness level (TL) is established in that for each trustworthiness level (TL) a different trustworthiness certificate (6) with a corresponding pair of participant public key (7) and participant private key (8) is used.

10. Method of establishing the trustworthiness level (TL) of a participant (2) in a communication connection between a first communication partner (1) and a second communication partner (3) and for adapting communication behaviour to the established trustworthiness level (TL), whereby said participant (2) is equipped with a securely stored participant private key (8) and that said first communication partner (1) performs an authentication test using said participant private key (8) which also leads to establishing said trustworthiness level (TL) and that in case of a successful authentication said first communication partner (1) communicates the established trustworthiness level (TL) to said second communication partner (3) and that at least one parameter of said communication behaviour is chosen in dependence of said established trustworthiness level (TL).
11. Method of establishing the trustworthiness level (TL) according to claim 10, characterized in that the authentication test is performed in that a test number (R_1) is transmitted by the first communication partner (1) to the participant (2) from where said test number (R_1) returns signed under use of the participant private key (8) and in that the signature of the returning test number (R_1) is verified by using a participant public key (7) which corresponds to said participant private key (8).

1/1

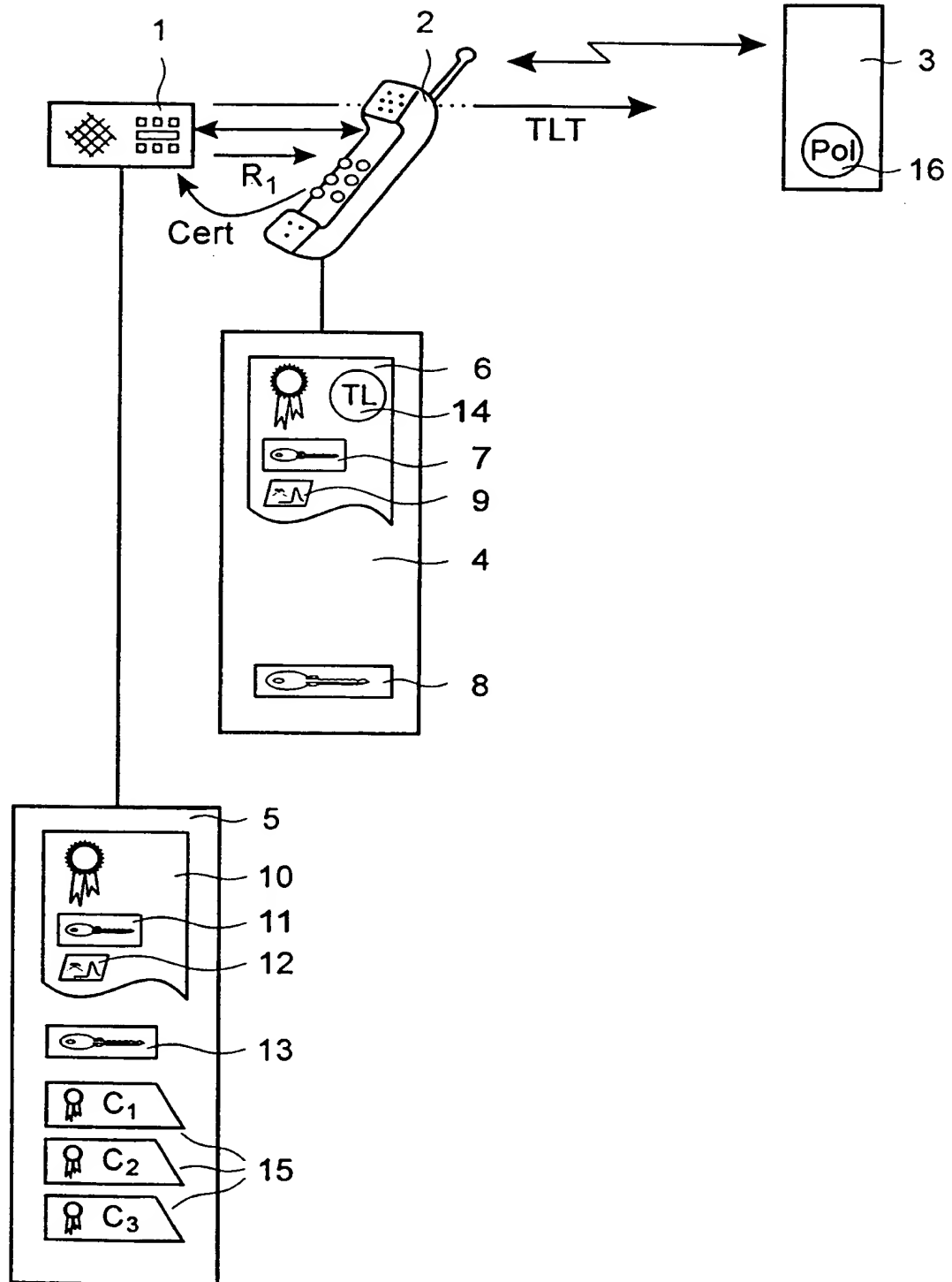


Fig. 1

INTERNATIONAL SEARCH REPORT

International Application No

PCT/IB 98/01854

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32 H0407/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MOLVA, SAMFAT AND TSUDIK: "Authentication of Mobile Users" IEEE NETWORK, vol. 8, no. 2, 1 April 1994, pages 26-34, XP000515077 NY, US	1-3
A	see page 30, line 1 - page 34, line 42; figures 3-6	4-9
Y	CHADWICK, YOUNG AND CICOVIC: "Merging and Extending the PGP and PEM Trust Models-The ICE-TEL Trust Model" IEEE NETWORK, vol. 11, no. 3, 1 May 1997, pages 16-24, XP000689785 NY, US	1-3
A	see page 21, line 54 - page 24, line 19; figures 3-5	4-9
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

16 March 1999

Date of mailing of the international search report

24/03/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.
Fax: (+31-70) 340-3016

Authorized officer

Geoghegan, C

INTERNATIONAL SEARCH REPORT

ational Application No

PCT/IB 98/01854

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 371 794 A (DIFFIE ET AL.) 6 December 1994	1-3
A	see column 3, line 46 - column 15, line 61; figures ---	4-9
A	US 5 402 490 A (MIHM, JR) 28 March 1995 see column 3, line 29 - column 12, line 49; figures ---	1-9
A	EP 0 586 022 A (FISCHER) 9 March 1994 see page 7, line 22 - page 20, line 51; figures ---	1-3
A	C PARK: "On Certificate-Based Security Protocols for Wireless Mobile Communication Systems" IEEE NETWORK, vol. 11, no. 5, 1 September 1997, pages 50-55, XP000699941 NY, US see page 51, line 1 - page 55, line 59; figures -----	1-3

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/IB 98/01854

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5371794 A	06-12-1994	EP 0651533 A JP 7193569 A	03-05-1995 28-07-1995
US 5402490 A	28-03-1995	NONE	
EP 586022 A	09-03-1994	US 5005200 A AT 113429 T AT 150605 T AU 620291 B AU 4242589 A CA 2000400 A,C DE 69013541 D DE 69013541 T DE 69030268 D DE 69030268 T DK 386867 T EP 0386867 A ES 2036978 T ES 2098651 T GR 93300050 T JP 2291043 A US 5214702 A	02-04-1991 15-11-1994 15-04-1997 13-02-1992 13-09-1990 07-09-1990 01-12-1994 09-03-1995 24-04-1997 26-06-1997 03-04-1995 12-09-1990 01-01-1995 01-05-1997 30-06-1993 30-11-1990 25-05-1993